IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,

Plaintiff,

vs. **Cr. No. 14-3761 JCH**

DONALD ALVIN TOLBERT,

Defendant.

MEMORANDUM OPINION AND ORDER

This matter is before the Court on three separate motions to suppress filed by the Defendant: (1) *Defendant's Motion to Suppress Evidence Seized Pursuant to September 20, 2012 Search Warrant at Defendant's Residence and Request for Evidentiary Hearing Under* Franks v. Delaware [Doc. 136], (2) *Defendant's Motion to Suppress Evidence Seized Pursuant to September 19, 2012 Search Warrants on America Online for Two E-Mail Accounts* [Doc. 137], and (3) *Defendant's Motion to Suppress Evidence Seized Pursuant to September 30, 2016 Search Warrants for Dell Dimension and eMachine Computers and Request for Evidentiary Hearing Under* Franks v. Delaware [Doc. 138]. In each motion, Defendant asks the Court to suppress evidence from a different aspect of the investigation in this case.

After reviewing each motion, the corresponding responses and replies, and the evidence cited by the parties, the Court concludes that all of the motions to suppress should be denied.

DISCUSSION

I. DEFENDANT'S MOTION TO SUPPRESS EVIDENCE SEIZED PURSUANT TO SEPTEMBER 20, 2012 SEARCH WARRANT [DOC. 136]

In this motion to suppress, Defendant Donald Tolbert ("Tolbert") argues that evidence that was discovered pursuant to a September 20, 2012 warrant to search his residence and possessions at 1021 4th Street SW ("The Dorm"), Albuquerque, New Mexico, should be suppressed because the warrant relied on an affidavit that contained recklessly false or misleading statements, as well as material omissions of fact, that undermine a finding of probable cause. Citing the Supreme Court's decision in *Franks v. Delaware*, Tolbert contends that there was no constitutional authority for the warrant. After reviewing the motion, response, and reply as well as the evidence provided by the parties, the Court concludes that the motion should be denied.

A. The Nature of a *Franks* Challenge

Under *Franks v. Delaware*, 438 U.S. 154 (1978), a Fourth Amendment violation occurs if (1) an officer's affidavit supporting a search warrant application contains a reckless misstatement or omission that (2) is material because, but for it, the warrant could not have lawfully issued. *See i*d. at 155-56; *United States v. Kennedy*, 131 F.3d 1371, 1376 (10th Cir. 1997). To win an evidentiary hearing to prove a *Franks* violation, a defendant must do more than allege a problem with the warrant. The Supreme Court has directed that a defendant's allegations "must be accompanied by an offer of proof.... Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained." *Franks*, 438 U.S. at 171; *see also Kennedy*, 131 F.3d at 1376. A court must strike any intentional, knowing, or reckless misstatements in the warrant application affidavit and assess the affidavit without them. 438 U.S. at 155-56. If instead the affidavit contains intentional, knowing, or reckless omissions, a court

must add in the omitted facts and assess the affidavit in that light. *Stewart v. Donges*, 915 F.2d 572, 582-83 (10th Cir. 1990).

B. *Franks* Does Not Apply

Tolbert's motion to suppress the evidence seized pursuant to the September 20, 2012 search warrant presents a different scenario than a typical *Franks* challenge. Usually, a defendant making a challenge under *Franks* asserts that the affiant who asked for the warrant placed false or misleading statements in the warrant affidavit in order to improperly induce a judicial officer to issue a search warrant. Here, Tolbert contends that the investigator first misled a grand jury in order to obtain a subpoena duces tecum to acquire evidence from third parties, and then relied on the improperly obtained evidence from those third parties in his affidavit in support of search warrant.

The warrant affidavit in question [Doc. 136-1] was signed by Special Agent Owen E. Pena of the New Mexico Attorney General's Office, Internet Crimes Against Children Task Force.[1] Tolbert contends that Pena gave false and misleading testimony before the state court's grand jury, which led the grand jury to issue subpoenas duces tecum for CenturyLink and America Online ("AOL"). *See* Doc. 136-3. The subpoena served on CenturyLink requested subscriber information for a particular IP address, "[i]ncluding the names(s) and addresses of the person(s) who opened the account, the date the account opened, detailed method of payment, telephone number(s) used

[1] For reasons that are not entirely clear to the Court, Tolbert attached as Exhibit 2 [Doc. 136-2] to his motion the Affidavit for Search Warrant supplied by Pena in support of the search warrant for a different location: 760 57th St. NW, Albuquerque, New Mexico, which is Tolbert's mother's address. Tolbert did not reside there. A close reading of Doc. 136 suggests that Tolbert is probably not challenging in this particular motion the constitutionality of the search of his mother's home, which makes Doc. 136-2 irrelevant to Doc. 136. However, the parties did not brief that issue, and consequently the Court will not address it here.

to access the Internet, email addresses, connection address, current/recent IP addresses, and any identifying information, which would tend to identify the person(s) subscribing to the service." Doc. 136-3 at 2. The subpoena duces tecum to AOL requested all the above information for the email addresses ddt123abc@aol.com and donnieisagod@aol.com (and their associated AOL screen names), as well as IP connection logs and "buddylist information." *Id*. at 1. Tolbert argues that Pena recklessly misled the grand jury into believing that Tolbert had committed a crime, Doc. 136 at 9-10, thereby causing the grand jury to issue subpoenas. He asserts that because Pena misled the grand jury, the information obtained through those subpoenas was obtained in violation of his constitutional rights. Tolbert argues that the information later obtained through the search warrants should be suppressed because the affidavit in support of the search warrant relied on information acquired through improperly obtained subpoenas.

Tolbert's argument fails because there is no authority to support an argument that *Franks* applies to testimony given before a grand jury or the resulting subpoenas. Tolbert cites no decisions in which a court has extended *Franks* beyond the context of a warrant affidavit, and the Court can find no case in which any federal court has applied a *Franks* analysis to grand jury testimony or to a subpoena. Perhaps this is because "the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated at the time of the subpoena is issued." *United States v. Miller*, 425 U.S. 435, 444 (1976).

To counter this argument, Tolbert relies upon *Carpenter v. United States*, 138 S. Ct. 2206 (2018). However, his reliance is misplaced. As the Court noted in its prior Memorandum Opinion and Order [Doc. 127 at 20-21], in *Carpenter* the FBI identified the cell phone numbers of several robbery suspects, and prosecutors were granted court orders to obtain the suspects' cell phone

records under the Stored Communications Act. These included a time-stamped record known as cell-site location information (CSLI) that is generated each time a phone connects to a cell site. These records generate an extremely detailed log of the phone's (and therefore the defendant's) physical locations and movements. Carpenter moved to suppress the data, arguing that the Government's seizure of the records without obtaining a warrant supported by probable cause violated the Fourth Amendment. The Court agreed, noting that there is a reasonable expectation of privacy in one's physical location. *Id*. at 2217. "Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled." *Id*. at 2216. The Supreme Court reasoned that before cell phones, police could follow a suspect for a short while, but doing so for an extended period of time was impractical and expensive, and therefore rare. *Id*. at 2217. As a result, Americans have come to expect that law enforcement would not and could not secretly monitor their movements for a long period of time. "Allowing government access to cell-site records contravenes that expectation," and "[m]apping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts" that provides the government with "an intimate window into a person's life." *Id*. Thus, the *Carpenter* court held that the government could not obtain such comprehensive, private information without a warrant. *Id*. at 2221.

The records that the grand jury in this case subpoenaed from CenturyLink and AOL are not like the CSLI records in *Carpenter*. The records in this case do not provide a detailed chronology of Tolbert's past movements over a period of time. Rather, they are more like the traditional business records in *United States v. Miller*, 425 U.S. 435 (1976) (no expectation of privacy in financial records held by a bank) and *Smith v. Maryland*, 442 U.S. 735 (1979) (no expectation of privacy in records of dialed telephone numbers conveyed to telephone company))

because they contain information about who the company's customers are, how long they have been using the company's services, and where they reside. This case is similar to the recently issued opinion in *United States v. Hood*, 920 F.3d 87 (1st Cir. 2019**)**, in which the First Circuit concluded that a defendant did not have a reasonable expectation of privacy in his IP address data acquired without a warrant from a smartphone messaging application and two internet service providers. The *Hood* court distinguished *Carpenter*, observing that an internet user generates the IP address data acquired in that case "only by making the affirmative decision to access a website or application. By contrast, as the Supreme Court noted in *Carpenter*, every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell tower without the cell phone user lifting a finger." *Id*. at 92. *See also United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018) (concluding that *Carpenter* analysis does not apply to IP address information obtained via grand jury subpoena from a smartphone messaging application). The information gathered in the grand jury subpoenas in this case does not provide comprehensive, detailed information about Tolbert's movements over an extended period of time. Rather, they are the type of records about a subscriber that are akin to the types of records kept by many businesses regarding the identities and locations of their customers. Further, the subpoenaed data appears to have been generated from Tolbert's own affirmative actions in utilizing CenturyLink and AOL, and in this way is distinguishable from the CSLI data in *Carpenter*. Thus, the information obtained from CenturyLink and AOL did not require a warrant.

In summary, Tolbert has failed to show that he has a reasonable expectation of privacy in the data that law enforcement obtained from CenturyLink and AOL. He has also failed to demonstrate that *Franks* and its progeny apply to grand jury testimony and grand jury subpoenas. For these reasons, his motion to suppress will be denied.

C. The Stored Communications Act

Tolbert argues that certain information requested by the grand jury subpoenas and then relied upon by Pena in his affidavit in support of search warrants was "outside the scope of what Congress authorized for disclosure by AOL in the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(c)(2) . . ." Doc. 136 at 10. Specifically, Tolbert alleges that "IP connection logs and buddylist information" exceed the scope of the statute—specifically, § 2703(c)(2)(E), which concerns the "instrument number of other subscriber number or identity, including any temporarily assigned network address." *Id*.; Doc. 151 at 3. Tolbert provides no explanation, reasoning, precedent, or authority for his position. Even if Tolbert is correct in his assertion that the Government violated the SCA, he provides the Court with no authority stating that suppression is the appropriate remedy. Further, he argues that IP connection logs and buddylists are more akin to the CSLI data in *Carpenter*. According to Tolbert, "IP connection logs specifically locate[] the user of an email address at an exact place and time, more specific and exact than the CSLI location information," and that in this day and age there is no way to avoid leaving behind this trail of data. Doc. 151 at 4.

In response, the Government argues that IP connection logs and buddylists are "implicitly included in the statute as collections of 'instrument number[s] or other subscriber number[s] or identity, including any temporarily assigned network address.'" Doc. 142 at 7. The Government also points to the lack of authority cited by Tolbert, *id*. at 7, and notes that in any event the information actually provided in the subpoena return does not include information about buddylists. *Id.* at 7-8, so the request for that information was immaterial.

The Court has already determined, *supra*, that Tolbert has failed to make even a preliminary showing that his Fourth Amendment rights were violated by the subpoenas and

subsequent search warrants. Tolbert has not shown that the SCA offers him greater protections than the Fourth Amendment. Accordingly, for this alternative reason his motion to suppress should be denied.

II. MOTION TO SUPPRESS EVIDENCE SEIZED PURSUANT TO SEPTEMBER 30, 2016 SEARCH WARRANTS FOR DELL DIMENSION AND eMACHINE COMPUTERS [Doc. 138]

Tolbert asks the Court to suppress evidence that was obtained during a September 30, 2016 search of two computers—a Dell Dimension and an eMachine—that had been found and seized by law enforcement when they searched his mother's home four years earlier, in September of 2012. Like the motion discussed above, this motion to suppress also relies upon *Franks*. Tolbert alleges that there were inaccuracies and material omissions in the Affidavit in Support of Application for Search Warrant [Doc. 138-1], which was signed by Special Agent Melva Boling of the United States Immigration and Customs Enforcement, Homeland Security Investigations. It appears from the record to be undisputed that Tolbert's mother, Margaret Tolbert, owned the two computers and that law enforcement seized them pursuant to a search of her home in September of 2012. It is also undisputed that Tolbert did not live in the home at the time of the search and seizure, nor did he own either computer.

The Government argues that Tolbert lacks standing to challenge the search of the two computers, which belonged to his mother and were seized during a search of her home. A "person has standing only to challenge the violation of his own Fourth Amendment rights." *United States v. Ladeaux*, 454 F.3d 1107, 1112 (10th Cir. 2006). "Fourth Amendment rights are personal, and, therefore, a defendant cannot claim a violation of his Fourth Amendment rights based only on the introduction of evidence procured through an illegal search and seizure of a third person's property or premises." *United States v. DeLuca*, 269 F.3d 1128, 1131 (10th Cir. 2001) (quotation omitted).

However, the Supreme Court has held that in some circumstances a person may have a legitimate expectation of privacy in someone else's home. For example, in *Minnesota v. Olson*, 495 U.S. 91 (1990) the Court decided that an overnight houseguest had the sort of expectation of privacy that the Fourth Amendment protects.

The relevant question presented here is whether defendant Tolbert "manifested a subjective expectation of privacy in the area searched and whether society is prepared to recognize that expectation as objectively reasonable." *United States v. Valdez Hocker*, 333 F.3d 1206, 1208-09 (10th Cir. 2003) (quotation omitted). It is Tolbert's "burden of demonstrating that he had a personal Fourth Amendment interest that was implicated by the search...." *United States v. Jones*, 213 F.3d 1253, 1260 (10th Cir. 2000).

In this case, the evidence shows that Defendant's mother, Margaret Tolbert, purchased the two computers and kept them at her home located at 760 57th Street NW in Albuquerque, New Mexico. *See* Margaret Tolbert testimony, Doc. 121, Transcript of June 12, 2018 hearing on motion to suppress, at pp. 10-15. Defendant Tolbert did not live in the home on 57th Street, nor was he permitted to stay there; rather, Margaret Tolbert lived alone. *Id*. at pp. 16-17. However, Defendant Tolbert did visit her house regularly to use her computers. *Id*. at p. 18. On September 20, 2012, law enforcement officers searched Margaret Tolbert's home pursuant to a search warrant and seized the two computers. Doc. 121 at pp. 15-16; Doc. 136-2. There is no evidence that Defendant Tolbert was present at his mother's home at the time of the search and seizure.

Defendant Tolbert argues that he had a subjective expectation of privacy in the emails he sent from his mother's computers and that his expectation of privacy was objectively reasonable. Tolbert fails to cite any authority that adequately supports his position. He turns, once again, to the Supreme Court's decision in *Carpenter v. United States*, but he fails to explain how his emails

that can be found on another person's computer in another person's home are entitled to the same level of privacy protection as the extensive, detailed location-tracking CSLI data discussed in that case. According to Tolbert, an email is the functional equivalent to a piece of physical correspondence, such as a letter—"a paper or effect for Fourth Amendment purposes," that is akin to "physical mail." Doc. 153 at 5-6. But again, he cites no authority to show that if law enforcement had found and searched copies of physical mail that he had previously sent from his mother's home, the outcome would have been any different.

By contrast, there is ample authority that supports the conclusion that Defendant Tolbert does not have a reasonable expectation of privacy in his mother's home and computers. The Supreme Court has stated that an overnight guest in a home may claim the protection of the Fourth Amendment, but one who is merely present with the consent of the householder may not." *Minnesota v. Carter*, 525 U.S. 83, 90 (1998). *See also United States v. Payne*, 99 Fed. Appx. 204, 208 (10th Cir. May 25, 2004) (unpublished) (one who was a frequent visitor to home, but not an overnight guest there, had no reasonable expectation of privacy in the premises). Here, Defendant Tolbert was not an overnight guest in Margaret Tolbert's home; he had not been permitted to stay there except for his first night out of jail. Doc. 121 at p. 17. Indeed, Defendant Tolbert was not even present in Margaret Tolbert's home at the time of the search. Thus, this case more closely resembles *United States v. Beckstead*, 500 F.3d 1154 (10th Cir. 2007), in which police searched the empty apartment rented by the defendant's girlfriend. *Id*. at 1157. Because there was no evidence that the defendant was living in the apartment or had even spent an occasional night there, the court concluded that he lacked a reasonable expectation of privacy in the apartment. *Id*. at 1164 (citing *United States v. Zermeno*, 66 F.3d 1058, 1061 (9th Cir. 1995) (holding that "mere fact that [the defendant] stored contraband at the … residence is insufficient to establish that he had a

legitimate expectation of privacy there")). *See also United States v. Dunning*, 312 F.3d 528, 532 (1st Cir. 2002) (defendant had no legitimate expectation of privacy in a house in which he had stayed occasionally in the past but in which he had no ownership or tenant rights, for which he did not have a key, and from which he had no right to exclude others); *United States v. Castro*, 225 Fed. Appx. 755, 758-59 (10th Cir. May 30, 2007) (unpublished) (concluding that defendant lacked standing to challenge the search of his girlfriend's apartment when the evidence showed he did not live there, his name was not on the lease, he kept no clothing there, he paid no bills for the apartment, and he was not present in the apartment at the time of the search). Because Defendant Tolbert did not live in his mother's home, did not regularly spend the night or pay bills there, and was not present at the time of the search, the Court concludes that he lacked a reasonable expectation of privacy in the home and its contents. Lacking standing to challenge the search of his mother's home, Tolbert also lacks standing to challenge the search of his mother's computers which were found inside her home. Thus, his motion to suppress the evidence found on those computers will be denied.

Because of the Court's conclusion on standing, it will not address the numerous other arguments[2] raised by the parties in their briefs.

III. DEFENDANT'S MOTION TO SUPPRESS EVIDENCE SEIZED PURSUANT TO SEPTEMBER 19, 2012 SEARCH WARRANTS ON AOL FOR TWO E-MAIL ACCOUNTS [DOC. 137]

[2] The Government also contends that Tolbert has failed to meet his burden to show the need for a *Franks* hearing, that there is a substantial basis on which to affirm the magistrate judge's finding of probable cause, and that the special needs, totality of the circumstances, inevitable discovery, and independent source exceptions to the warrant requirement apply. For the reasons described herein, the Court need not reach these arguments.

Tolbert moves to suppress all evidence obtained through a search of two email accounts, donnieisagod@aol.com and ddt123abc@aol.com, on September 19, 2012. [Doc. 137] Special Agent Christina Altamirano of the United States Immigration and Customs Enforcement, Homeland Security Investigations, searched his accounts by virtue of two warrants that she obtained from a United States magistrate judge. Tolbert argues that the searches of those accounts violated his constitutional rights because the warrants authorizing those searches were invalid. Specifically, he contends that the federal magistrate judge from the District of New Mexico who issued the warrants lacked authority to do so because the warrant applications and supporting affidavits contained no facts or evidence to show that the crimes being investigated took place in New Mexico, thereby failing to demonstrate on their face that the magistrate judge had jurisdiction to issue the warrants. Thus, Tolbert argues that the warrants did not satisfy Fed. R. Crim. Pro. 41 and the SCA, and therefore were invalid under the Fourth Amendment.

In response [Doc. 144], the Government argues that Rule 41 and the SCA do not require a warrant affidavit to include facts establishing territorial jurisdiction. Second, the Government contends that it required no warrant to search Tolbert's email accounts because he lacked a legitimate expectation of privacy in his emails due to the terms of his probation and his own violation of AOL's terms of service, as well as the fact that AOL performed a private search of his emails before the warrant was even issued. Third, the Government argues that various exceptions to the warrant requirement apply in this case, including special needs, totality of the circumstances, good faith, and inevitable discovery.

A. The Magistrate Judge's Jurisdiction to Issue the Warrant

The two warrants and their supporting applications, attachments, and affidavits, which can be found at Doc. 137-1, are virtually identical. Attachment A to both warrants provides that the

items to be seized include, inter alia, "[a]ll electronica mail and attachments to electronic mail . . . contained in, or on behalf of" the two email addresses listed above. Doc. 137-1 at 4 of 26. It also provides that "the search warrant will be presented to AOL personnel." *Id*. Attachment B to both warrants, which contains a description of the property to be searched, states: "AOL is a free and subscriber-based e-mail service provided with its primary computer information systems and other electronica communications and storage systems, records, and data located in Northern Virginia." Doc. 137-1 at 6 of 26.

Tolbert argues that the two warrants are invalid because they do not demonstrate on their face that the magistrate judge had authority to issue the warrants. He points to Federal Rule of Criminal Procedure 41(b)(1), which provides that magistrate judges have the authority to issue search and seizure warrants only for persons or property located within the judge's district. He contends that the warrants at issue here do not satisfy Rule 41(b)(1) because they were issued by a magistrate judge in the District of New Mexico for email accounts stored in Northern Virginia. However, Tolbert acknowledges that the Stored Communications Act provides an exception to this rule when a search warrant is issued for the content of electronic communications "using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction[.]" 18 U.S.C. § 2703(a)-(b). The statute defines a "court of competent jurisdiction" as "any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals *that has jurisdiction over the offense being investigated*." 18 U.S.C. § 2711(3)(A)(i) (emphasis added). This allows a judge issuing a search warrant for the contents of electronic communications under the SCA to extend beyond the reach of his or her jurisdiction, provided that the underlying offense being investigated took place within that judge's jurisdiction. As a result of the foregoing, Tolbert contends that the two warrants issued for the contents of the

two AOL email addresses were invalid because the applicant, Agent Altamirano, failed to show in the supporting documentation that the crimes being investigated took place within the District of New Mexico.

Tolbert does not dispute that the crimes of which he is accused, and which Agent Altamirano was investigating when she applied for the warrants, allegedly took place in New Mexico. He has not challenged the jurisdiction of the District of New Mexico in this case, nor has he argued that New Mexico is not the proper venue for its adjudication. Thus, Tolbert does not suggest that the magistrate judge *actually lacked* jurisdiction to issue the two warrants in question—rather, he contends that the warrants are defective because the supporting applications, attachments, and affidavits do not demonstrate facts supporting the magistrate judge's jurisdiction.

In support of his argument, Tolbert relies upon a decision from our sister court in the District of Kansas, *United States v. Barber*, 184 F. Supp.3d 1013 (D. Kan. 2013). In *Barber*, the defendant challenged warrants issued by magistrate judges in Maryland for information that Google stored in California regarding a particular Gmail account. *Id*. at 1015-16. Ultimately, investigators discovered that the Gmail address was associated with the defendant at a physical address in Kansas. *Id*. at 1016. As a result, the case was prosecuted in the District of Kansas. *See id*. at 1015. After discussing Rule 41(b) and the relevant provisions of the SCA extending a judge's jurisdiction to issue a warrant, the *Barber* court made an observation upon which Tolbert heavily relies: "The government presented no evidence that the offense being investigated occurred in Maryland." *Id*. at 1017. The court then made a second statement that Tolbert largely ignores, concluding that the Maryland magistrate judge "lacked jurisdiction to issue the second warrant *because the offense being investigated did not take place in Maryland*." *Id*. at 1018 (emphasis

added). As a result, the *Barber* court held that the warrant was void from its inception due to lack of jurisdiction. *Id*.

In both *Barber* and this case, the warrant issued by the magistrate judge contained no information to support a conclusion that the offense being investigated occurred in the magistrate judge's own judicial district. However, this case is distinguishable from *Barber* in one crucial respect: the magistrate judge in this case did, in fact, have territorial jurisdiction to issue the warrants because the offense being investigated actually did take place in New Mexico, the same state where the warrants were issued. There is no evidence in the record to dispute that fact. However, that was not the case in *Barber*, in which the crimes being investigated were committed in Kansas, but the warrant was issued by a Maryland magistrate judge. Thus, we see the importance of the *Barber* court's second statement, *supra*—that the warrant in that case was void *from its inception* because the Maryland magistrate judge never had jurisdiction, not because of the contents of the warrant, but because the crimes being investigated took place outside of his jurisdiction. That is simply not the case here. The alleged crimes being investigated by Agent Altamirano took place in the District of New Mexico, which Tolbert does not dispute. That fact, though not clear from the face of the warrant, is still true. Thus, the magistrate judge in this case had jurisdiction and the warrants were not void *ab initio* for lack of jurisdiction.

Tolbert seems to suggest that the warrants are invalid not because the magistrate judge actually lacked jurisdiction, but rather because the warrants failed to show on their face the factual basis for his jurisdiction. While it may be ideal practice for an affiant to include in the warrant facts supporting the judge's jurisdiction to issue the warrant, the Court can find no authority that requires the warrant affidavit to contain such facts. Nothing in the Fourth Amendment, Rule 41, or the SCA demands that a warrant or its supporting documents contain this information.

Furthermore, Tolbert points to no such requirement in either the Fourth Amendment, Rule 41, or the SCA. The Court will not impose an additional requirement where none exists. Although the warrant and warrant affidavit do not show the basis of the magistrate judge's jurisdiction, that absence cannot negate the fact that he did have jurisdiction.

The motion to suppress on the grounds that the warrant was invalid should be denied.

B. <u>The Private Search Doctrine</u>

Even if the magistrate judge's warrant were invalid for lack of jurisdiction, the motion to suppress still should be denied because the private search doctrine—an exception to the warrant requirement—applies in this case.

Under the private search doctrine, "the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant's expectation of privacy has not already been frustrated." *United States v. Runyan*, 275 F.3d 449, 461 (5th Cir. 2001). Under the doctrine, the defendant's privacy previously has been breached by a private actor who is not bound by the Fourth Amendment, thereby diminishing the invasion of privacy that occurs when a government actor later repeats the same search. The Supreme Court's decision in *United States v. Jacobsen*, 466 U.S. 109 (1984), explains the proper analysis. In *Jacobsen*, employees of Federal Express observed that one of its packages had been damaged in transit. They opened the package and discovered a white powder. In response, the employees contacted the Drug Enforcement Administration, whose agents conducted chemical field tests on the white powder and determined that the power was cocaine. The government then used the test results to obtain a warrant and arrest the package's intended recipients, who subsequently challenged the government's actions as unconstitutional. The Supreme Court held that the agents' actions did not violate the Fourth Amendment. "Once frustration of the original expectation of privacy occurs, the

Fourth Amendment does not prohibit governmental use of the now-nonprivate information." *Id*. at 117. Any expectation of privacy the recipients might have had in the package's contents was abrogated when the Federal Express employees opened and searched the package and discovered the white powder. The government's subsequent use of that information—its test to discern the powder's chemical composition—infringed no expectation of privacy that had not already been infringed.

The question presented here, then, is whether, by the time Agent Altamirano viewed the suspect image files, Tolbert's expectation of privacy in his computer files had already been thwarted by searches conducted by AOL, a private third party. The Government argues that AOL had already viewed the emails and attachments at issue before the Government executed its search warrant. *See* Doc. 144 at 12. The evidence in this case shows that under its usual business practice, AOL conducted a private search of Tolbert's emails very soon after submitting a CyberTip to the National Center for Missing and Exploited Children ("NCMEC"). Mark Ludlow, currently an employee of Oath, Inc. (into which AOL was subsumed) and an employee of AOL during the relevant time period, testified that when AOL's IDFP (image detection filtering process) software detects an email containing suspected child pornography being sent through its system, its practice is to close the account and send a report to NCMEC. Then, an AOL employee opens and views both the email and all of its attachments to determine if they contain child pornography. *See* Mark Ludlow testimony, Transcript of April 25, 2018 hearing on motion to suppress, at pp. 5, 7-8, 14-15, 18, 35. The private search of the intercepted email and attachment generally occurs one business day after it is flagged by AOL's IDFP system. Gregory Phillips testimony, Doc. 121, Transcript of June 12, 2018 hearing at pp. 122, 129-130.

In light of this testimony, the Court concludes that there is more than sufficient evidence to conclude that AOL opened and viewed Tolbert's emails (which were dated July 17, 2012; August 7, 2012; and September 1, 2012; respectively) and the attached images before the September 19, 2012 warrant was executed. Each of these emails generated a CyberTip report because AOL's IDFP system detected a hash value match with something in AOL's database that has previously been determined to be child pornography. Thus, each of these emails will have been subject to the AOL process described above, which includes opening and viewing the emails and their attachments. This private search by AOL effectively diminished Tolbert's expectation of privacy in those files before they were viewed by Agent Altamirano.

The Fifth Circuit reached a similar conclusion in *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018). In that case, the defendant uploaded files to SkyDrive, a cloud hosting service. *Id*. at 637. When he did so, Microsoft's PhotoDNA program (which, like AOL's IDFP, automatically scans the hash values of user-uploaded files) reviewed the hash values of those files and compared them against its existing database of known child pornography hash files. *Id*. at 639. When PhotoDNA detected a match, it created a CyberTip and sent the file to NCMEC. *Id*. at 638. The Fifth Circuit interpreted this as a private search by Microsoft that frustrated whatever expectation of privacy the defendant might have had in the hash values of his files. *Id*.

Unlike Tolbert's files in this case which were first opened and viewed by AOL, the files of the defendant in *Reddick* were not opened by Microsoft; instead, they were merely scanned for a hash value match before being sent along to NCMEC and then eventually to the police. It was the police who first opened and viewed the files. *Id*. at 638, 639. Despite this, the Fifth Circuit held that when the police detective opened the files, "there was no significant expansion of the search that had been conducted previously by a private party sufficient to constitute a separate search."

Id. at 639 (internal citations and quotations omitted). The Fifth Circuit reasoned that the officer's actions in opening the files merely confirmed that the flagged files were indeed child pornography, as expected. *Id*.

Here, the private search by AOL went much further and included, as per its usual business practice, an AOL employee opening and viewing Tolbert's flagged emails and attachments. Thus, there can be no doubt that Tolbert's expectation of privacy in those files was frustrated by AOL, a private party, before law enforcement viewed the files and confirmed their content. Thus, the private search doctrine applies. For this alternate reason, the motion to suppress will be denied.

IT IS THEREFORE ORDERED that:

(1) *Defendant's Motion to Suppress Evidence Seized Pursuant to September 20, 2012 Search Warrant at Defendant's Residence and Request for Evidentiary Hearing Under* Franks v. Delaware [Doc. 136] is **DENIED**;

(2) *Defendant's Motion to Suppress Evidence Seized Pursuant to September 19, 2012 Search Warrants on America Online for Two E-Mail Accounts* [Doc. 137] is **DENIED**; and

(3) *Defendant's Motion to Suppress Evidence Seized Pursuant to September 30, 2016 Search Warrants for Dell Dimension and eMachine Computers and Request for Evidentiary Hearing Under* Franks v. Delaware [Doc. 138] is **DENIED**.

UNITED STATES DISTRICT JUDGE